IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

A Novel Conceptual Solution for Security Enhancement in Internet of Things

Madhavi Gudavali[1*], Vidyasree P[2], Viswanadha Raju S[3]

[1] Department of CSE, UCEN JNTUK Narasaraopet, Andhra Pradesh, India
[2] Department of CSE, Stanley Women's Engineering College and Research Scholar of JNTUH, Hyderabad, Telangana, India
[3] Department of CSE, JNTUH CEJ, Hyderabad, Telangana, India

[*]*Corresponding Author: madhavi.researchinfo@gmail.com, Tel.: 9908194643*

Available online at: www.ijcseonline.org

Accepted: 05/Jun/2018, Published: 30/Jun/2018

Abstract— Internet of Things (IOT) makes the smart devices eventually as stepping stones for cyber-physical smart pervasive framework development. IOT is a dynamic global network infrastructure where large amount of information is being transferred through network with interoperable communication protocols. Research and innovation is being carried out in the areas of IOT on semantic interoperability, cyber-physical system, security, and various network technologies. Security is the major challenge among these different areas in the fields of IOT. In this paper, we propose a new conceptual solution to enhance the security in IOT applications based on the feature level fusion of iris and fingerprint biometric traits through deep learning feature extractor Extreme Learning Machine (ELM). Forward Error Correction (FEC) is employed on the fused multimodal biometric traits to encrypt and secure the biometric data.

Keywords—Extreme Learning Machine; Internet of Things; Information; Multimodal Biometrics; Security

I. Introduction

Internet of Things is a network of different physical objects to interact with internal states or external environment [1]. It confluences different technologies, effective wireless protocols, interoperable communication protocols, cheap processors and efficient secured methods to build a smart environment. These advancements attracted the researchers to construct a smart world by assembling real, digital and virtual environments that create energy, cities, health-care, transport and other areas more intelligent. The key idea behind IOT is to facilitate the things to be connected with anyone, anytime, anywhere through any network and utilize any technology to reach the common goal. It is a global dynamic network framework where different objects recognize themselves and they attain intelligence through facilitating things to be connected through anywhere-anytime approach. Information is transferred through the internet where the security is the major challenge.

Multimodal biometrics addresses the security issues in very efficient way. Iris biometric has the high stability rate and cannot be compromised easily [2]. Finger print biometric is the universal trait with unique features to identify an individual. Biometrics is incorporated within the smart devices to authenticate the user and to secure the information over the network. It addresses the problems like loss of control, loss of trust and multi tenancy. Research has been done to integrate the unimodal biometrics like fingerprint recognition system within the smart devices for user authentication but unfortunately this system also got compromised and information got hacked. Fingerprint recognition system has more benefits at the same time it has certain drawbacks. User is certified as unauthenticated if he has dirt, grease, cuts and contaminated content on his/her finger.

Multimodal biometrics address the unimodal biometric issues very effectively and efficiently [3]. It fuses two or more traits like face, finger, iris and palm etc, of an individual into a single trait [4]. Fusion can be performed at various levels like sensor level, feature level, match score level and decision level. These fusions provide the high level of authentication and privacy for users' biometric data. The motivation behind the proposed system is to attain high secure authentication over the network and proposed system performance is amplified through Extreme Machine Techniques [5]. Forward Error Correction accomplishes more privacy that encrypts biometric data when it is employed on the fused feature map of iris and fingerprint traits. Therefore, in this paper, we proposed feature level fusion of iris and finger print recognition system through Extreme Machine Learning (ELM) [6][7]. ELM helps to classify and extracts the features of the individual traits to maximize the recognition rate of an

individual [8]. The rest of the paper is organized as follows- Section 2 demonstrate the security issues in the fields of IOT. Section 3 illustrates the proposed methodology and finally, Section 4 concludes the paper.

II. IOT Security Issues

IOT confluences different technologies, effective wireless protocols, interoperable communication protocols and efficient secured methods to build smart environment applications. Security is the major concern in IOT environment[9]. Huge amount of transactions, highly confidential data are transferred via internet to the connected devices. High end security is needed from the initial layer of the IOT system [10]. Security concerns expanded with the expansion of internet to protect financial transactions, privacy data and other information as it is not separable from safety. Network security issues are addressed to some extent through firewall protection, intrusion detection and prevention system and other security systems [11]. Antivirus, malware detection techniques, black listing and also advanced techniques like white listing techniques are also incorporated for the security but unfortunately some of these techniques also got compromised by the intruders. Advanced access control mechanisms are implemented on the corporate network to authenticate the individual and the devices. In recent years, the major concern is about authentication of an individual and protecting the information. These techniques are applied in IOT, which requires large amount of reengineering process to reach or satisfy the device constraints[12]. The major challenges in the fields of IOT are

- Pervasive data collection
- High end user authentication
- Potential for unexpected uses of user data
- High security and safety

Multimodal biometrics addresses some of the security challenges in IOT through amplifying the high end authentication of user recognition when it is incorporated within the smart device.

III. Methodology

IOT is a global dynamic network framework where smart devices are interconnected with each other to exchange the information via network. Multi modal biometric readers are incorporated with the smart devices to achieve the high end authentication. Multimodal biometrics combines different modalities or traits to authenticate an individual. The proposed system demonstrated in "Fig 1" illustrates the feature level fusion of iris and finger print biometrics to amplify the authentication and recognition accuracy of the user. The sobel operator is used for preprocessing of the finger print and Gabor filter is employed on iris to eliminate the noises and other illuminations. ELM is employed on both iris and fingerprint to extract the rich features individually. Feature level fusion is accomplished on iris and fingerprint feature maps to generate template with rich feature map of an individual which is used for high end authentication. FEC is employed on the fused feature map for encrypting fused template so as to minimize the attacks against stored templates.

Step 1: Image Acquisition

The iris and face images are acquired and are transformed into grayscale for pre-processing.

Step 2: Preprocessing

The preprocessing phase eliminates various distortions and noises of two traits. Gabor filter is applied on iris to eliminate the unwanted data like eye lashes, eye lids and other noises. Sobel operator is employed on fingerprint image to avoid dirt, grease and other noises. Both techniques help to preserve the unique properties of iris and fingerprint data.

Step 3: Feature Extraction through ELM

Extreme Learning Machine is employed on the individual preprocessed traits of iris and fingerprint. Unique features are extracted from both iris and fingerprint biometrics with a unified learning platform. It is used for multi-class classification and unlike traditional learners; hidden features are obtained randomly by ELM learner prior to training data. The hidden features are unique to every individual and also independent to it and to other features.

Hidden features are trained through ELM and $f(y)$ is an activation function to learn P different samples formulated in (1). In the activation function of ELM, weights and biases are generated randomly to make non-linear system as linear. f_{ji} is the output of j^{th} hidden feature with respect to y_i, w_j is weight vector connected with j^{th} hidden features and input features, while b_j is the bias of j^{th} hidden feature. X is the desired output feature vector of both individual iris and fingerprint.

$$X=\sum_{j=1}^{P} \beta_j \cdot f(w_j * y_i + b_j) \quad (1)$$

Step 4: Feature Level Fusion

Horizontal concatenation method is employed to combine the heterogeneous extracted feature sets of iris and fingerprint features. This fusion reduces the feature space through solidified template [9].

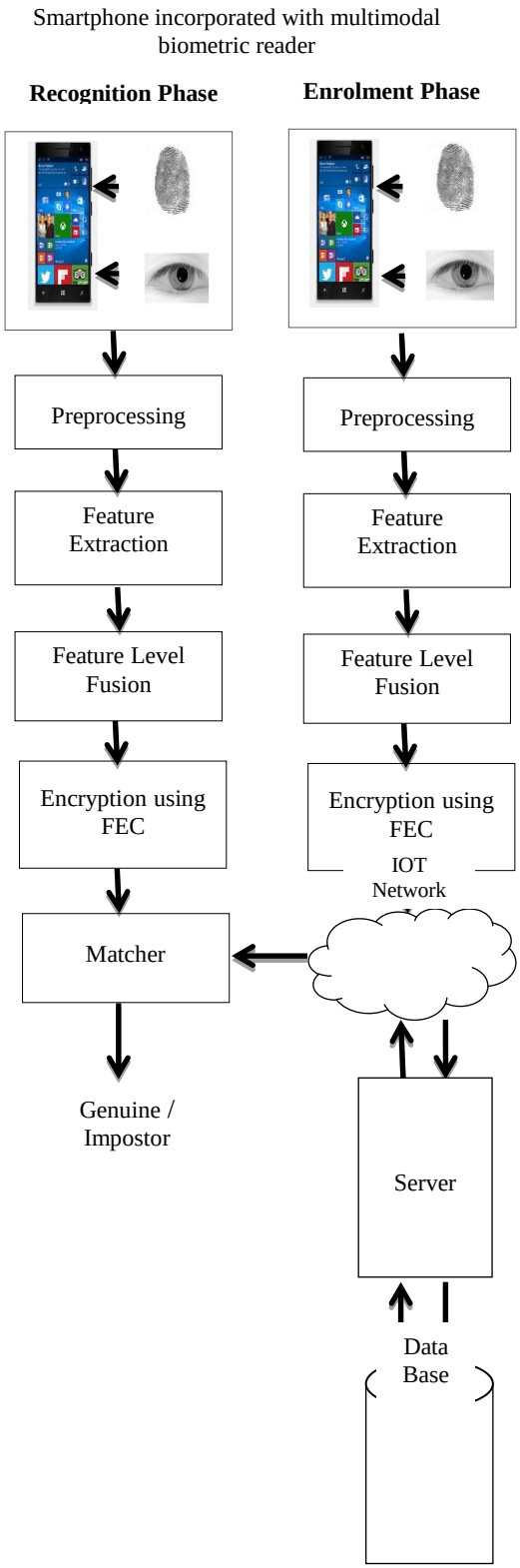

Figure 1: Architecture of Proposed Multimodal Biometric Recognition System in IOT

Step 5: Encryption of fused feature template using FEC
Forward Error Correction technique is employed on the fused feature vector map to encrypt the template data of iris and finger print traits. Feature fused vector map is transformed using FEC by adding the noisy data that achieves the cancel ability concept. This encrypted template cannot be compromised by the intruders with in a specific time period. FEC technique helps in denoising the data and also error correction. It consummates the security, protection on confidential data and safeguards from content corruption. This fused encrypted feature vector is transferred via network and stored in either database or network storage devices. Matching is performed to authenticate the individual as impostor or authenticated user.

IV. Conclusion

IOT is a dynamic global network infrastructure where large amount of information is being transferred through network with interoperable communication protocols. Security is the major concern in IOT. Multimodal biometrics incorporated within the smart devices address the security issues of IOT applications as it has high stability over unimodal recognition systems. The proposed system demonstrates the feature level fusion of iris and fingerprint for accurate authentication of the user. ELM is applied on pre-processed images to extract the unique features of iris and fingerprint traits. Feature level fusion is done to integrate the extracted features of iris and fingerprint traits and then fused feature space is reduced through FEC. This FEC technique encrypts the fused biometric template and provides security as well as privacy for stored templates along with demographic information over network devices. Convolution Neural Network can be incorporated in the proposed recognition system to further achieve high level security in IOT through multimodal biometrics.

References

[1] L. Mainetti, L. Patrono, and A. Vilei, "*Evolution of wireless sensor networks towards the Internet of Things: A survey*" in Proc. 19th Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM), pp. 1_6, Sep. 2011.

[2] Dr.Madhavi Gudavalli, Dr.S.Viswanadha Raju, Dr.A.VinayaBabu and Dr.D.Srinivasa Kumar, "*MultiModal Biometrics-Sources, Architecture & Fusion Techniques: An Overview*", IEEE-International Symposium on Biometrics and Security Technologies (ISBAST'12), Taipei, Taiwan, March 26-29, 2012.

[3] SubhashV.Thul, AnuragRishishwar, NeeteshRaghuwanshi, "*Sum Rule Based Matching Score Level Fusion of Fingerprint and Iris Images for Multimodal Biometrics Identification*", International Research Journal of Engineering and Technology (IRJET), Volume: 03, Issue.02, Feb 2016.

[4] Ashraf Aboshosha, Kamal A. El Dahshan, Eman A. Karam, Ebeid A. Ebeid, "*Score Level Fusion for Fingerprint, Iris and Face*

Biometrics", International Journal of Computer Applications by IJCA Journal, Volume 111 - Number 4, DOI: 10.5120/19530-1171, 2015.

[5] Erik Cambria, Guang-Bin Huang, Liyanaa rachchi Lekamalage ChamaraKasun, Hongming Zhou, Chi Man Vong, Jiarun Lin, Jianping Yin, ZhipingCai, Qiang Liu, "*Extreme Learning Machines Trends & Controversies*", IEEE Intelligent Systems, DOI: 10.1109/MIS.2013.140, Volume: 28, Issue: 6, pp. 30-59, Feb 2014.

[6] Dr.S.Viswanadha Raju, P.Vidyasree, Dr.Madhavi Gudavalli "*Reinforcing The Security In India's Voting Process Through Biometrics",* International conference on Advanced computer science and information technology, Chennai September 2014.

[7] S.N.Deepa, B.Arunadevi, "*Extreme learning machine for classification of brain tumor in 3D MR images*", Informatologia, Vol.46 No.2, http://hrcak.srce.hr/106430, Jun 2013.

[8] Zhiyong Huang, Yuanlong Yu, Jason Gu, Huaping Liu, "*An Efficient Method for Traffic Sign Recognition Based on Extreme Learning Machine*", IEEE Transactions on Cybernetics, DOI: 10.1109/TCYB.2016.2533424, Volume: PP, Issue: 99,pp. 1-14, Mar 2016.

[9] P.Vidyasree, Dr.S.ViswanadhaRaju, Dr.Madhavi Gudavalli, "*Desisting The Fraud In India's Voting process through Multi modal Biometrics*",IEEE 6th International Conference on Advanced Computing 2016.

[10] J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, "*From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*", Amsterdam, The Netherlands: Elsevier, 2014.

[11] Gurpeet Kaur, Manreet Sohal, "*IOT Survey: The Phase Changer in Healthcare Industry*" International Journal of Scientific Research in Network Security and Communication, Vol.6, Issue 2, April 2018.

[12] Anusha Bharati, Ritika Thakur, Kavita Mhatre, "*Protection of Industrial and Residential areas by Wireless Gas Leakage Detector using IOT and WSN*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.3, pp.62-67, June 2017.

[13] National Highway Traffic Safety Administration, "*Traffic safety facts 2012*," DOT HS 812 012, U.S. Department of Transportation, April 2014, pp. 42.

Authors Profile

Dr.Madhavi Gudavalli received B.Tech(CSIT) from JNTU , M.Tech(CSE) and Ph.D in Computer Science & Engineering discipline from JNTU Hyderabad. She is currently working as Assistant Professor in the department of Computer Science and Engineering at JNTUK University College of Engineering Narasaraopet. She is guiding/guided many projects in the areas of image processing, computational intelligence and machine learning for UG, PG and Ph.D students of CSE & IT Departments. Her research interests are in the areas of Biometrics, Pattern recognition, Image Processing, Deep Learning, Cloud and IoT security. Her research articles are accepted in international Conferences and journals and proceedings are published in IEEE, Springer, ACM digital libraries. She is the member of editorial boards, technical committees of IEEE international conferences and peer-reviewed international journals. Her research ideas are protected through four Patents in biometrics, cloud computing and embedded systems domains which are published in Indian Patent Journal. She played a vital role in AICTE-NBA Accreditation work at CVR college of Engineering, Hyderabad in 2007. She is conducting/conducted several workshops, seminars and conferences at institutional level. She was sanctioned with Major Research Project entitled A Next Generation Identity Verification System to Provide Security in the area of Biometrics as Co-Principal Investigator by AICTE under Research Promotion Scheme. In recognition of her outstanding scientific contributions her research articles received Travel grant from DST and UGC. She is a Life member in different Professional bodies such as ISTE, CSI and fellow member of IEEE. Her research contributions are not only confined to subject area but also extended to other related domains arising out of the new education system, assessment and accreditation, and their impact on Indian Higher Education. As an off shot of research endeavour's her papers were accepted and presented in World Education Summit (WES 2012-AICTE) entitled *International Practices In Assessment, Accreditation & Quality Standards In Higher Education*, ICTIEE- 2014 Poster entitled *The Institutional Leadership of JNTUK System in Embracing New Paradigms in Engineering Education* and IEEE-IACC 2016 entitled *Role of ICT in Outcome Based Education.* The hallmarks of her illustrious career include teaching Engineering and Technology and pursuing exemplary research on improving security by using advanced technologies and tools.

Vidyasree P pursed Bachelor of Technology from University of JNTUK, in 2013 and Master of Technology from JNTUH University in the year 2015. She is pursuing Ph.D(CSE) and working as Assistant Professor in the department of Computer Science and Engineering at Stanly college of Engineering since 2015. She is a member of IEEE. She has published more than 10 research papers in reputed international journals including ACM and IEEE. Her main research work focuses on Biometrics and Internet of Things. She has 2 years of teaching experience and 1 year of Research Experience.

Dr. S.Viswanadha Raju working as Professor of Computer Science and Engineering department at CEJ, JNTUniversity Hyderabad. He is a distinguished academician whose advanced research work in the field of Programming in C, Information Retrieval, Data Mining, Biometric Systems and Research Methodology are globally recognized. He filed THREE patents deriving from his research and also received awards from various bodies on the basis of his contribution. He was sanctioned with two Major Research Projects by AICTE under Research Promotion Scheme. He has been granted funds from national organizations such as Dept. of Science and Technology (DST), AICTE, UGC etc to encourage research on his domains. He has given several invited talks and tutorials in Research Methodology, Programming tips, Algorithms, Information Retrieval, Data mining, Biometrics and relevant areas. He visited Singapore and Taiwan to attend international conference for presenting research work and he received Travel grant from UGC. he is the life member of IETE, ISTE, CSI and IACSIT. He guiding or guided more than 42 students/scholars: Ph.D., (12) and M.Tech/MCA (29) besides guiding a large number of student projects. He is credited with 50 research publications in National and International journals repute. His research contributions are not only confined to his subject area but also extend to other related domains arising out of the new education system, assessment and accreditation, and their impact on Indian Higher Education. To add impetus to his academic credentials he has undergone training for the quality improvement in education at NITTTR, WOSA-2012, TCS, Infosys, and NBA etc. He conducted an International Conference on Advanced Computing Technologies 2008 with the capacity of Convener. He served as Head of dept of CSE at JNTUHCEJ and also as Director of MCA (Accredited by NBA) and proceeding to this served as a Head of the Dept of CSE/MCA (CSE- Twice accredited by NBA) at GRIET.He initiated and actively participated in AICTE approval, accreditation (NBA) , NAAC and TEQIP work etc. he played a instrumental roles in organizing various conferences , seminars, workshops and acted as convener, coordinator,etc.

